

**AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT & ARREST WARRANT**

I, Brendan C. Fogerty, having been duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since January 2015. I am currently assigned to the Violent Crimes and Major Offender Unit in the Boston Field Office of the FBI, where my responsibilities include the investigation of violent crimes, including crimes related to extortion. I have gained experience through training at the FBI Academy, post Academy training, and everyday work related to conducting these types of investigations.

2. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. I am currently conducting an investigation into activity in violation of Title 18, United States Code, Section 875(d)¹ (extortion). Based on evidence discovered throughout the course of this investigation, there is probable cause to believe that James F. Connor, V (“**CONNOR**”), who currently resides in West Chester, Pennsylvania, violated Title 18, United States Code, Section 875(d) by transmitting communications via Twitter and text message threatening to publicly disseminate naked pictures of a person if

¹ Title 18, United States Code, Section 875(d) states as follows: Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

she did not accede to his demands to, among other things, provide him with additional nude and sexually explicit images.

4. The information contained in this Affidavit is based upon my personal observations during the course of this investigation, on information conveyed to me by other law enforcement officials, and on my review of records, documents, and other physical evidence obtained during this investigation. Because this Affidavit is being submitted for the limited purpose of securing a criminal complaint and arrest warrant, I have not included each and every fact known to me concerning this investigation, but instead have set forth only the facts necessary to establish the requisite probable cause.

5. The events described herein occurred in the District of Massachusetts and elsewhere.

DEFINITIONS

6. The following are definitions related to the Internet, social media, and other computer tools as they apply to the activity discussed in this Affidavit²:

a. FaceTime: FaceTime is a real-time video chatting application developed by Apple, Inc. Through the application users can conduct one-on-one video calls between Apple products such as iPhones, iPads, iPod Touches, and Mac notebook and desktop computers. To use the application, users must register with Apple and create an Apple ID.

b. Internet: The Internet is a collection of computers, computer networks, and devices that are connected to one another via high-speed data links and telephone lines for the purpose of communication and sharing data and information. Connections

² The definitions provided here are based on my training and experience, as well as other sources, including research and discussions with other agents.

between Internet-enabled computers and devices exists across state and international borders; therefore, information sent between two devices connected to the Internet frequently crosses state and international borders even where the two devices are located in the same state.

c. Internet Protocol (“IP”) Address: An IP address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 128.195.188.231). Every computer connected to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most Internet Service Providers control a range of IP addresses.

d. Internet Service Provider (“ISP”): Many individuals and businesses obtain access to the Internet through businesses known as ISPs. ISPs provide their customers with access to the Internet using telephone or telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISP’s servers; remotely store electronic files on their customers’ behalf; and may provide other services unique to the particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. These records often include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, and other information both in computer data and written record format.

e. Snapchat: Snapchat is a video messaging application through which users can take photos, record videos, and send them to a controlled list of recipients. These

sent photographs and videos are known as “Snaps.” Users set a time limit (ranging from 1 to 10 seconds) for how long the recipients can view their Snaps, after which they are purportedly deleted.

f. Tumblr: Tumblr is a web logging platform and social networking website that allows users to post multimedia and other content to a short-form web log (also known as a “blog.”). Users can follow other users’ blogs, as well as make their blogs private.

g. Twitter: Twitter is an online social networking service that enables users to send and receive short 140 character messages. These messages are known as “Tweets.” To use the service, individuals must register and create user accounts. All Twitter account names, which are also known as “handles,” begin with an “@” symbol. The service also allows users to follow one another. Twitter also offers messaging services through which users can send and receive private messages that exceed 140 characters. These messages are sometimes referred to as “Direct Messages” or “DMs.” Tweets and Twitter Direct Messages are transmitted between users through the Internet.

STATEMENT OF PROBABLE CAUSE

7. On September 22, 2015, VICTIM³, date of birth XX, XX, 1996, a sophomore at a university within the District of Massachusetts, reported to university police that she was being harassed and extorted via text messages and social media by **CONNOR**. According to VICTIM, **CONNOR** threatened to send VICTIM’s family and social media contacts photographs of her in the nude and performing sexual acts, unless she complied with his demands, which included, among other things, sending him

³ The true name of the victim is known to law enforcement but is not included in the Affidavit for confidentiality purposes.

additional naked pictures through Snapchat, masturbating in front of him using FaceTime, and breaking up with her current boyfriend.

8. VICTIM reported that she met **CONNOR** through Tumblr in 2012 and developed an online relationship with him. They have never met in person. She stated that when she met **CONNOR**, he claimed to be suicidal. VICTIM explained that she communicated with him over a long period of time in order to help him work through those problems. Over the course of her communications with **CONNOR**, VICTIM reported that she sent nude photos to him using Snapchat. According to VICTIM, **CONNOR** somehow preserved the images before they were deleted by the application. It is these images that VICTIM reports **CONNOR** has threatened to release to her family and other contacts.

9. As part of the investigation, I obtained and reviewed records from the Pennsylvania Department of Motor Vehicles and discovered that **CONNOR** was issued Driver's License number [REDACTED]. According to **CONNOR**'s driver's license records, his date of birth is XX/XX/1995 and he currently resides in West Chester, Pennsylvania.

10. On September 25, 2015, I interviewed VICTIM at her university police department in Boston, Massachusetts. In addition to the information provided to university police, VICTIM reported the following:

a. She met **CONNOR** online when she was a sophomore in high school. Her parents did not approve of the online relationship and instructed her to end it. Despite her parents' instructions, VICTIM continued communicating with **CONNOR** because he reported being suicidal and she wanted to help him. Early on in the relationship, **CONNOR** used the threat of suicide to coerce VICTIM to do things such as

quit school clubs he did not approve or return home from sleepovers at her friends' homes.

b. She has communicated with **CONNOR** various ways since meeting him, including via: (i) telephone at [REDACTED] 1475; (ii) email at [REDACTED]@comcast.net; (iii) Twitter at @[REDACTED]; (iv) Snapchat at [REDACTED]; (v) FaceTime at [REDACTED] 1475; (vi) Facebook; (vii) Tumblr; and (viii) Kik Messenger.

c. Around approximately late-2012/early-2013, VICTIM and **CONNOR's** online relationship turned romantic and she and **CONNOR** frequently used Snapchat and FaceTime to send naked photographs and/or perform sexual acts on video in front of each other. At first, this was consensual; however, around approximately Spring 2013, **CONNOR** began forcing VICTIM to send naked pictures and engage in sexual video chats against her will by threatening to tell her parents that they were still in a relationship. VICTIM was afraid her parents would find out and complied with **CONNOR's** demands.

d. **CONNOR** preserved many of the Snapchat images and FaceTime video chats without telling VICTIM. VICTIM later learned **CONNOR** had done so because he threatened to post the images online. **CONNOR** threatened to disseminate or post naked pictures of VICTIM on several occasions. On at least one instance, **CONNOR** sent VICTIM a screenshot of the images ready for submission to the website www.collegefession.com, a website marketed as an anonymous social sharing platform for college students, which features a photo gallery section purportedly containing photographs of college girls.

e. In Fall 2014, VICTIM entered her freshman year in college and continued occasional communications with **CONNOR**. Around approximately Spring 2015, **CONNOR** told VICTIM that if she agreed to send him five sexually explicit images and videos over a five-week period, he would permanently delete the images. VICTIM agreed to do so.

f. Around approximately Summer 2015, VICTIM informed **CONNOR** that she no longer wanted any type of relationship with him. **CONNOR** reportedly became upset and at one point during a telephone call with VICTIM, he threatened to rape her.

g. Approximately 1-2 weeks ago, VICTIM informed **CONNOR** that she was in a relationship with another person and **CONNOR** became upset and aggressive. That is when the current threats to release the images began. **CONNOR's** most recent extortionate demands include: (i) maintaining contact with **CONNOR**; (ii) VICTIM agreeing to a similar picture/video sharing arrangement as the one he demanded in the Spring 2015; and (iii) VICTIM ending the relationship with her current boyfriend.

h. Although **CONNOR** has engaged in this type of extortionate and threatening behavior in the past, this time was different because **CONNOR** went as far as Direct Messaging three of her Twitter followers and told them he has pictures confirming that she is cheating on her new boyfriend with **CONNOR**. Among the Twitter followers messaged by **CONNOR** were VICTIM's fifteen year-old cousin, another male university student, and a male from VICTIM's high school class with whom she has not communicated since graduating.

11. During the September 25, 2015 meeting with VICTIM, she provided me with access to her telephone and social media accounts. Review of VICTIM's phone and

social media accounts revealed that the majority of the threatening communications were sent to VICTIM primarily via Twitter.

12. In particular, I reviewed the Direct Messages sent by Twitter user @ [REDACTED] to VICTIM. In them, @ [REDACTED] confirmed that he in fact did still possess the sexually explicit photos of VICTIM and he threatened sending them to her parents and Twitter followers. Throughout the conversation, @ [REDACTED] appears to become upset when VICTIM refuses to accede to his demands and at one point, in addition to threatening to release the pictures, he alludes to physically injuring her as well.

13. For example, on or about September 18, 2015, @ [REDACTED] threatened to release the photos unless she ended the relationship with her boyfriend. When VICTIM refused, @ [REDACTED] became increasingly agitated writing *“YOU ARE ALREADY IN DEEP SHIT. YOU CAN CONTINUE PLAYING ME AND STALLING, BUT ENOUGH IS ENOUGH. IF YOU DON’T WANT TO BE RUINED, I SUGGEST YOU AGREE[.] IM DONE FUCKING PLAYING GAMES[.]”*⁴ VICTIM implored @ [REDACTED] to *“please leave [her] alone[.]”* at which point he threatened to drive to Boston and go on a *“GO ON A RAMPAGE”* if she did not give in. @ [REDACTED] then sent VICTIM a screenshot image of a map depicting the route from West Chester, Pennsylvania to Boston with the phrase *“Here I come!”*

14. Later that day, @ [REDACTED] sent VICTIM a series of Direct Messages explaining that he had already contacted some of her Twitter followers and he threatened

⁴ With the exception of redactions to protect the identity of VICTIM, all Direct Messages referenced in this Affidavit have been reproduced exactly as they were sent by @ [REDACTED] including spelling errors and letter case.

to contact her parents. He also sent a screenshot of a Whitepages listing for VICTIM's mother containing her name, address, and phone number.

15. Throughout that day, September 18, 2015, @ [REDACTED] continued messaging VICTIM, but she did not respond. That evening, he said *"You should message me back...And I do have hard evidence against you...CALL ME PLEASE."* @ [REDACTED] then sent VICTIM a picture of a photo array containing 16 sexually explicit photos of VICTIM. The picture of the sexually explicit photo array revealed that the images were displayed on a computer monitor. @ [REDACTED] also stated *"I did block the people I messaged, but I could unblock them and show them this as hard evidence, and don't think I won't. If your boyfriend gets any whiff of this, you are gonna be dumped. Try me. So you can either end it with him and continue to talk to me, or this is shared as hard evidence. Your choice!"*

16. VICTIM also received numerous threatening telephone text messages that day from several unknown telephone numbers. At approximately 11:23 PM, VICTIM received a text message from telephone number [REDACTED] 4345 stating *"You should check Twitter. I am offering a peace offering. But I could also turn sour as I have something on you that you don't think I do."*

17. Later that night, at approximately 11:50 PM, VICTIM received a text message from telephone number [REDACTED] 1965 stating *"I wouldn't do a damn thing [VICTIM]."* The message also included a web address to a website that once clicked on showed the same 16 picture array of sexually explicit photos of VICTIM and stating *"Want this to be shared to the people I messaged? If your boyfriend gets wind of this, you are dumped[.]"*

18. Still later that evening, at approximately 11:59 PM, VICTIM received a text message from telephone number [REDACTED] 4124 stating *"I'm done playing games. Talk to me. Call me[.] At my cell number[.] Or I release that pic tonight."*

19. On or about September 21, 2015, VICTIM informed **CONNOR** that she was going to seek help from law enforcement because she felt he was lying and manipulating her, and would not delete the images as he had promised on prior occasions.

20. On or about September 22, 2015, VICTIM told **CONNOR** that her parents had contacted an attorney⁵. According to VICTIM, at that point **CONNOR** became even more agitated and his threats and demands increased. Now, in addition to demanding that VICTIM end her relationship, he also demanded that she recant what she told her parents and he further conditioned not releasing the sexually explicit images on VICTIM sending him additional sexually explicit images and masturbating in front of him via video chat.

21. The threatening Twitter Direct Messages also escalated. For example, on or about September 22, 2015, @ [REDACTED] sent VICTIM another screenshot of the sexually explicit 16-photo array and stated *"I knew you would pull this! This is why I kept them! I'm not an idiot. Unless you fix this, they are being shared[.] I'm not playing games anymore. Go to the cops do whatever[.] I don't care[.] If what you told me was true, then I have nothing to lose here, so play your cards wisely, because I am pressing send here shortly[.]"*

⁵ Neither VICTIM nor her parents actually contacted an attorney regarding **CONNOR**. According to VICTIM, she represented to **CONNOR** that they had in order to get him to stop threatening and extorting her.

22. @ [REDACTED] then sent VICTIM additional screenshots of the same 16-picutre array ready to send to people VICTIM knew including her minor cousin.

VICTIM reminded @ [REDACTED] that she was a minor when those images were taken and that if he disseminates them, he would be distributing child pornography.

@ [REDACTED] responded by saying *"I don't care[.]"* As the Direct Message exchange continued, VICTIM told @ [REDACTED] that it made her uncomfortable to do the things he was demanding she do, to which @ [REDACTED] responded *"Well, swallow the bullet or other guys are gonna see you naked[.] I'm done playing. You crossed a huge line this evening and I'm done. This one is on you now. 3 minutes[.] 2 minutes[.] Clock is ticking[.] 1 minute[.]"*

23. VICTIM eventually capitulated and represented to @ [REDACTED] via Twitter Direct Message that she spoke to her mother and a lawyer was no longer involved. At that point @ [REDACTED] sent VICTIM his additional demands which included, among other things, that she send him five sexually explicit pictures and have five sexually explicit video chat sessions per week over a five week period.

@ [REDACTED]'s demands also required that two of the video chat sessions occur while she is in school. Finally, @ [REDACTED] also demanded that he get to observe VICTIM while she urinates.

24. Over the next several days, @ [REDACTED] continued to press for sexually explicit images and imposed deadlines for VICTIM to share pictures and videos with him. On or about September 26, 2015, @ [REDACTED] demanded that VICTIM begin sending him sexually explicit images that evening between certain hours. VICTIM delayed @ [REDACTED] by telling him that she did not any time constraints imposed and

asking him to be patient. @██████████ responded with yet another threatening ultimatum stating “*You agree, and follow through, or the pics are sent out.*” VICTIM implored @██████████ to stop, but he was undeterred – forcefully responding “*We are doing sexy snaps and everything tonight or the pics are sent out. You will follow through[.] I’m done playing games[.]*”

Linking CONNOR to the Criminal Activity

25. During the course of this investigation, I have linked this criminal activity to **CONNOR** in several ways.

26. As part of the investigation, I located several social media accounts that appear to belong to **CONNOR** including, Facebook⁶ and Tumblr⁷. Both of these account pages, which were open and accessible to the public, contained the same profile picture and listed the account owner as either “JC” or “James Connor.”

27. I also reviewed the webpage corresponding with the Twitter account @██████████, which is open and accessible to the public. As stated above, this is the account that VICTIM reports **CONNOR** used to communicate with her during their relationship and the account from which the threatening communications originated. On the biographical portion of the page, @██████████ indicates that he is located in West Chester, Pennsylvania. I compared the individual depicted in @██████████’s profile photo (which is identical to the profile photos on the aforementioned Facebook and Tumblr pages) and, based on a comparison with **CONNOR**’s Pennsylvania Driver’s License, it is the same person.

⁶ <https://www.facebook.com/people/██████████>

⁷ <http://██████████.tumblr.com/>

28. On September 27, 2015, Twitter responded to a request for basic subscriber and IP address login information related to the Twitter account @ [REDACTED]. According to this information, account [REDACTED], which uses the handle @ [REDACTED] was created on July 6, 2012 by a user from IP address 76.98.9.95. Further investigation regarding IP address 76.98.9.95 revealed that it resolved back to Comcast Cable Communications, Inc. ("Comcast") as the ISP.

29. The Twitter records for @ [REDACTED] also indicated that telephone number [REDACTED] 1475 and email address [REDACTED]@comcast.net are associated with @ [REDACTED].

30. Review of law enforcement and public records databases revealed that telephone number [REDACTED] 1475 is an active AT&T wireless telephone number registered to James Connor at the same address as is reflected on **CONNOR's** Pennsylvania Driver's License. Also, the email address [REDACTED]@comcast.net is the same email address VICTIM reported using to communicate with **CONNOR** in the past.

31. The Twitter records for user @ [REDACTED] also included recent IP address login information from September 25, 2015 through September 27, 2015. Among the IP addresses listed was 76.98.9.95, the same Comcast IP address from which the @ [REDACTED] account was created.


32. On September 28, 2015, I spoke with a Comcast representative with regards to a request for subscriber information associated with IP address 76.98.9.95 and for email address [REDACTED]@comcast.net. According to the Comcast representative, the referenced IP and email addresses are registered to James Connor at the same address as is reflected on **CONNOR's** Pennsylvania Driver's License.


CONCLUSION

33. Based on the foregoing, I respectfully submit there is probable cause to conclude that **CONNOR** has committed and is continuing to commit extortion, in violation of Title 18, United States Code, Section 875(d).


BRENDAN C. FOGERTY,
SPECIAL AGENT, FBI

SUBSCRIBED and SWORN to before me
this 29th day of September 2015, in Boston, Massachusetts.


DAVID H. HENNESSY
UNITED STATES MAGISTRATE JUDGE



-